



Iran-linked APT TA453 targets Windows and macOS

CRITICALITY

12/07/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

The Iranian APT “TA453”, that targets Middle East and US, sends a spear-phishing email that is disguised as a pleasant conversation starter and focuses on foreign policy. In addition, emails are sent requesting feedback on the project "Iran in the Global Security Context" as well as authorization to submit a draft for review.



Threat Details

In a recent campaign that included malware for both Apple and Microsoft systems, researchers reported that hackers backing the Iranian regime were aiming their attacks at nuclear security and affairs experts of Middle East and US.

TA453 is a threat organization associated with Iran's Islamic Revolutionary Guard Corps (IRGC) that has been active at least since 2011. It is also known by the aliases APT35, Charming Kitten, Mint Sandstorm, and Yellow Garuda. The adversary's usage of CharmPower (also known as GhostEcho or POWERSTAR), an upgraded version of a PowerShell implant, was recently exposed by Volexity.

The spear-phishing email poses as a friendly conversation starter with a focus on foreign policy emphasis. The email stated that the researchers were seeking input from professionals for a project they were working on called "Iran in the Global Security Context." The hackers claimed the project was being worked on by other well-known nuclear security professionals to support its credibility. Prior to this, the attackers had also sent emails pretending to be those individuals. Even offering to pay the expert for their analysis of the paper, the hackers. Additionally, the emails asked for feedbacks on a project titled "Iran in the Global Security Context" and requested permission to provide a draft for review.

The researchers discovered that the TA453 was distributing a new infection chain intended for the deployment of a new PowerShell backdoor known as GorjolEcho by leveraging a range of cloud hosting providers.

In addition, the threat actors first exchanged a benign email with the target recipient before sending a malicious link that leads to a Google Script macro. After the macro has been run, the recipient is taken to a Dropbox URL. A password-protected.rar file called "Abraham Accords & MENA.rar" was hosted at the given URL. The "Abraham Accords & MENA.pdf.lnk" dropper could be found inside the.rar archive. It is important to note that the use of an LNK file and a.rar archive for malware dissemination differs from the conventional infection chain for TA453, which includes remote template injection or VBA macros. The PowerShell downloads more stages from a cloud hosting service after opening the included LNK file.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

Greig, J. (2023, July 6). *Iran-based hackers targeting nuclear security experts through Mac, Windows malware*. Retrieved from The Record: <https://therecord.media/iran-ta453-apt42-charming-kitten-espionage-nuclear-security-think-tanks>

Paganini, P. (2023, July 8). *Iran-linked APT group tracked TA453 has been linked to a new malware campaign targeting both Windows and macOS systems*. Retrieved from Security Affairs: https://securityaffairs.com/148275/apt/ta453-malware-windows-macos.html?utm_source=dlvr.it&utm_medium=twitter



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Center recommends all the entities to follow the below steps:

- Educate users on malware threats, train your users on techniques that can help them avoid social engineering schemes, such as phishing attacks, and report suspicious communication or system behavior to the security team.
- Strong passwords and software updates, ensure all users create strong, unique passwords, and regularly change passwords. Use a password manager to make it easier for users to use and remember secure passwords. Update your systems as quickly, as security flaws become known and patches are released.
- Back up your data and your test restore procedures, backup is a critical practice that can help to protect against data loss. It can help ensure that normal operations can be maintained even if the organization is attacked by network-based ransomware worms or other destructive cyber attacks.
- Partition your network, you should use network segmentation to isolate important parts of your network from each other. This can significantly reduce the “blast radius” of successful attacks, because attackers will be limited to a specific network segment and cannot move laterally to other parts of the network.
- Implement a layered security approach, including a secure email solution, a company-sanctioned file-sharing solution, and endpoint protection on user devices.
- Continuously monitor network traffic.



Appendix B – Detection

Type	Value
IP Addresses	• 144[.]217[.]129[.]176
Files	• mena.rar • encrypted.rar • a.rar • a.txt • id.txt
MD5	• ddead6e794b72af26d23065c463838c385a8fdff9fb1b8940cd2c23c3569e43b
Domain	• filemanager[.]theworkpc[.]com • fuschia-rhinestone[.]cleverapps[.]io • library-store[.]camdvr[.]org



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)



CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
- Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
- MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

RED

For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

GREEN

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction